https://doi.org/10.33778/kcsa.2020.20.1.009

Analysis of Variants of the Even-Mansour scheme

HongTae Kim*

요 약

There have been many papers on minimalism of cryptography. Secure minimal block cipher is one of these topics and Even and Mansour suggested a simple block cipher. The Even-Mansour scheme is a block cipher with one permutation and two whitening keys. Studying related to the Even-Mansour scheme gives great insight into the security and design of block cipher. There have been suggested many trials to analyze the security of the Even-Mansour scheme and variants of the Even-Mansour scheme. We present a new variant of the Even-Mansour scheme and introduce a variant of the Even-Mansour scheme. We focus on the security of these variants of the Even-Mansour scheme and present variation of the security according to key size. We prove the security of a variant of the Even-Mansour scheme and show that a generalized Even-Mansour scheme is not proper for a minimal block cipher.

이븐-맨서 스킴의 변형된 스킴에 관한 분석

김 홍 태*

ABSTRACT

암호학에서 최소화에 관한 많은 연구가 이루어지고 있다. 안전한 최소의 블록암호는 이러한 연구주제 중의 하나이며, 이븐(Even)과 맨서(Mansour)는 간단한 블록암호를 제안하였다. 이븐-맨서 스킴은 하나의 치환(permutation)과 두 개의 표백화키(whitening key)를 갖는 일종의 블록암호이다. 이븐-맨서 스킴에 관련된 연구는 블록암호의 안전성과 설계에 대한 이해에 큰 도움을 준다. 이븐-맨서 스킴과 이의 변형된 스킴의 안전성을 분석하기 위한 많은 시도들이 제안되어 왔다. 우리는 이븐-맨서 스킴의 새로운 변형된 스킴을 제시하고 기존의 변형된 스킴을 소개한다. 우리는 이븐-맨서 스킴의 변형된 스킴의 안전성에 초점을 맞추고 키의 크기에 따르는 안전성의 변화를 제시한다. 우리는 이븐-맨서 스킴의 변형된 스킴의 안전성을 증명하고 일반화된 이븐-맨서 스킴이 최소의 블록암호로 적합하지 않음을 보인다.

Key words : Minimalism, Analysis, Even-Mansour scheme, Block cipher, Security

접수일(2020년 02월 27일), 수정일(1차: 2020년 03월 16일), 게재확정일(2020년 03월 26일)

* 공군사관학교/수학과

1. Introduction

There have been many topics related to minimal concept in cryptography. For example, these are cryptographic assumptions, key sizes, scheme structures [16]. Even and Mansour proposed a block cipher having one permutation and two whitening keys [12, 13]. This scheme shows that we can make a block cipher with very simple structure. Of course, we should consider how to make the permutation. There have been presented papers about analyzing the security of the Even-Mansour scheme [7, 4, 10]. The scheme came into the limelight as the minimality of block ciphers was important. Some variants of the Even-Mansour scheme and security analysis on those schemes were lately proposed [1, 3, 5, 6, 8, 9, 11, 14, 15]. These are about the security analysis as numbers of permutation and key size increase.

Though there have been suggested many studies on the security according to the increase of permutation number and key size, studies on the security with respect to key size only are not presented enough. We only focus on the security of variants of the Even-Mansour scheme according to the increase of key size. We show that a variant of the Even-Mansour scheme with four keys we present has the same increase ratio of the Even-Mansour scheme in the security as the variant scheme increases from the Even-Mansour scheme in the key size. Biryukov et al. introduced a variant of the Even-Mansour scheme called a generalized Even-Mansour scheme [2]. According to Biryukov et al., we know that the generalized Even-Mansour scheme gets huge increase of key size according to small increase of attack complexity.

2. Main Result

Let F be a permutation on $\{0,1\}^n$. The Even-Mansour scheme $EM: \{0,1\}^n \rightarrow \{0,1\}^n$ is given as follows [12, 13]:

$$EM^F_{k_1,k_2}(P) = F(P \oplus k_1) \oplus k_2 \qquad (1)$$

where k_1,k_2 are keys chosen at random from $\{0,1\}^n$, P is a plaintext from $\{0,1\}^n$ and $\oplus$ denotes exclusive OR operation. In short, we write Equation (1) as $E(P) = EM^F_{k_1,k_2}(P) = F(P \oplus k_1) \oplus k_2$. Even and Mansour showed that to attack the Even-Mansour scheme needs $O(2^{\frac{n}{2}})$ plaintext/ciphertext pairs from Definition 2.1 and Theorem 2.1.

Definition 2.1 ([13]) The existential forgery problem is to find a new pair (P,C) such that $E(P) = C$; i.e., a pair which does not consist of a query and an answer, as previously supplied by either the E-oracle or the E^{-1}-oracle.

Let s and t be the number of E/E^{-1} queries and the number of F/F^{-1} queries, respectively.

Theorem 2.1 ([13]) The probability of an algorithm A to solve the existential forgery problem, when F and $K=(k_1,k_2)$ are chosen randomly and uniformly, is bounded by $O\left(\frac{st}{2^n}\right)$.

2.1 A variant of the Even-Mansour scheme

We introduce a variant of the Even-Mansour scheme and examine the number of plaintext/ciphertext pairs needed to attack the scheme. A variant of the Even-Mansour scheme $VEM: \{0,1\}^{n} \rightarrow \{0,1\}^{n}$ we present is given as follows:

$$VEM^{F}_{k_1,k_2,k_3,k_4}(P) = k_3 F(k_1 P \oplus k_2) \oplus k_4 \qquad (2)$$

where k_1,k_2,k_3,k_4 are keys chosen at random from $\{0,1\}^{n}$, P is a plaintext from $\{0,1\}^{n}$ and $\oplus$ denotes exclusive OR operation.

The above scheme consists of one permutation and four keys. We get the number of plaintext/ciphertext pairs to attack the variant of the Even-Mansour scheme using similar method of Theorem 2.1′s proof.

Theorem 2.2 The probability of an algorithm A to solve the existential forgery problem on the variant of the Even-Mansour scheme in the Equation (2), when F and $K=(k_1,k_2,k_3,k_4)$ are chosen randomly and uniformly, is bounded by $O\left(\frac{st}{2^{2n}}\right)$.

Proof. Define two sets S and T such that

$$S = \{(P_i, C_i), (\widetilde{P}_i, \widetilde{C}_i) | i = 1,2,\cdots,s\}$$

and

$$T = \{(X_i, Y_i), (\widetilde{X}_i, \widetilde{Y}_i) | i = 1,2,\cdots,t\}$$

where $E(P_i) = C_i, E(\widetilde{P}_i) = \widetilde{C}_i, F(X_i) = Y_i$ and $F(\widetilde{X}_i) = \widetilde{Y}_i$. We say that subkeys (k_1,k_2) are bad with respect to sets S and T if there exist i,j such that $k_1 P_i \oplus k_2 = X_j$ and $k_1 \widetilde{P}_i \oplus k_2 = \widetilde{X}_j$. Otherwise, (k_1,k_2) is good with respect to S and T. Similarly, we say that subkeys (k_3,k_4) are bad with respect to sets S and T if there exist i,j such that $k_3 Y_i \oplus k_4 = C_j$ and $k_3 \widetilde{Y}_i \oplus k_4 = \widetilde{C}_j$ and (k_3,k_4) is good with respect to sets S and T otherwise. The key $K=(k_1,k_2,k_3,k_4)$ is good with respect to S and T if (k_1,k_2) and (k_3,k_4) are good. A pair (K,F) is consistent with respect to S and T if for any pair (P_i, C_i), $(\widetilde{P}_i, \widetilde{C}_i)$ in S, we have $C_i = k_3 F(k_1 P_i \oplus k_2) \oplus k_4$, $\widetilde{C}_i = k_3 F(k_1 \widetilde{P}_i \oplus k_2) \oplus k_4$ and for any pair (X_i, Y_i), $(\widetilde{X}_i, \widetilde{Y}_i)$ in T, we have $F(X_i) = Y_i$, $F(\widetilde{X}_i) = \widetilde{Y}_i$.

First of all, we show that for all S,T, the probability

$$Pr_{K,F}[K=k \,|\, (K,F) \text{ is consistent with } S,T]$$

is the same for any good key $k \in \{0,1\}^{4n}$ with respect to S,T. It is enough to show that

$$p = Pr_{K,F}[(K,F) \text{ is consistent with } S,T \,|\, K=k]$$

is the same for any good key $k \in \{0,1\}^{4n}$ with respect to S,T. Given a good key $k=(k_1,k_2,k_3,k_4)$, we can transform (P_i, C_i), $(\widetilde{P}_i, \widetilde{C}_i)$ in S to $(k_1 P_i \oplus k_2, k_3^{-1} C_i \oplus k_3^{-1} k_4)$, $(k_1 \widetilde{P}_i \oplus k_2, k_3^{-1} \widetilde{C}_i \oplus k_3^{-1} k_4)$, respectively and get a new set U of set S. Since the key k is good, $S \cap U = \varnothing$. Therefore the probability p is the probability that F has $s+t$ distinct input/output pairs and hence does not depend on k.

The second step shows that the probability of an algorithm A to solve the existential forgery problem on the variant of the Even-Mansour scheme is bounded above. We show this using two probabilities. These are the probability p_α that a query will cause a good key to become a bad key and the probability p_β that the algorithm A can generate a new consistent pair (P,C) given the key is still a good key. Since the number of bad keys about (k_1,k_2) and the number of bad keys about (k_3,k_4) are both at most st, the number of good keys is at least $2^{4n} - 2st2^{2n}$. Thus the probability p_α is bounded by

$$\frac{2st2^{2n}}{2^{4n} - 2st2^{2n}} = O\left(\frac{st}{2^{2n}}\right).$$

Since both $F(k_1 P_i \oplus k_2)$ and $F(k_1 \widetilde{P_i} \oplus k_2)$ can be possible for $2^n - s - t$ values, the probability p_β is

$$\frac{1}{(2^n - s - t)^2} = O\left(\frac{st}{2^{2n}}\right).$$

Therefore the probability of the algorithm A to solve the existential forgery problem is bounded by $O\left(\frac{st}{2^{2n}}\right)$. □

We get the result that the security of this variant of the Even-Mansour scheme increases to $O(2^n)$ from $O(2^{\frac{n}{2}})$ of the Even-Mansour scheme as the key size increases to 2^{4n} from 2^{2n}. For $n = 128$, key size of the Even-Mansour scheme is 256 bit in contrast to the variant of the Even-Mansour scheme's key size 512 bit and the security of the Even-Mansour scheme is 2^{64} in contrast to the variant of the Even-Mansour scheme's security 2^{128}. The security and key size of the former scheme is simultaneously the square of those of the latter.

<Table 1> Key size and security of the Even-Mansour scheme and the variant of the Even-Mansour scheme(EM: the Even-Mansour scheme, VEM: the variant of the Even-Mansour scheme)

Plaintext/ ciphertext size	Key size		Security	
	EM	VEM	EM	VEM
128 bit(n = 128)	256 bit	512 bit	2^{64}	2^{128}
192 bit(n = 192)	384 bit	768 bit	2^{96}	2^{192}
256 bit(n = 256)	512 bit	1024 bit	2^{128}	2^{256}

2.2 The generalized Even-Mansour scheme

The generalized Even-Mansour scheme $GEM: \{0,1\}^n \to \{0,1\}^n$ is given as follows [2]:

$$GEM^F_{A_1, A_2, k_1, k_2}(P) = A_2 F(A_1 P \oplus k_1) \oplus k_2 \qquad (3)$$

where A_1, A_2 are keys chosen at random from $\{0,1\}^n \to \{0,1\}^n$ linear transformations and others are like Equation (1).

Biryukov et al. showed that they can get the key of the generalized Even-Mansour scheme with $O(n^3 2^{2n})$ complexity using affine equivalence [2]. Though the key size of the generalized Even-Mansour scheme increases to 2^{2n^2+2n} from 2^{2n} of the Even-Mansour scheme, the complexity of this generalized scheme increases to $O(n^3 2^{2n})$ from $O(2^{\frac{n}{2}})$. The complexity of the generalized Even-Mansour scheme is roughly the fourth power of that of the Even-Mansour scheme as the key size of the former is roughly the n-th power of that of the latter scheme. For $n = 128$, the security of the generalized Even-Mansour scheme is 2^{277} in contrast to the scheme's expectation security $2^{8,256}$. The generalized Even-Mansour scheme is very inefficient from the above. The security of the generalized Even-Mansour scheme is not proved yet.

<Table 2> Key size and security of the Even-Mansour scheme and the generalized Even-Mansour scheme(EM: the Even-Mansour scheme, GEM: the generalized Even-Mansour scheme)

Plaintext/ ciphertext size	Key size		Security	
	EM	*GEM*	*EM*	*GEM*
128 bit(n = 128)	256 bit	33024 bit	2^{64}	2^{277}
192 bit(n = 192)	384 bit	74112 bit	2^{96}	$2^{406.75}$
256 bit(n = 256)	512 bit	131584 bit	2^{128}	2^{536}

3. Conclusion

Even and Mansour suggested a minimal block cipher and many studies on this scheme have been presented. We analyzed the security of variants of the Even-Mansour scheme. The variant of the Even-Mansour scheme with four keys has the security 2^{128} from the Even-Mansour scheme's security 2^{64} as the key size of the former is 512 bit from the latter's key size 256 bit. When we design a block cipher, the generalized Even-Mansour scheme is not appropriate compared with the original Even-Mansour scheme. This is because the key size has increased significantly from 256 bit to 33024 bit for $n=128$. It would be interesting to attack the variant of the Even-Mansour scheme with four keys and to analyze the security of the generalized Even-Mansour scheme.

References

[1] E. Andreeva, A. Bogdanov, Y. Dodis, B. Mennink and J. P. Steinberger, "On the Indifferentiability of Key-Alternating Ciphers", Proceedings of CRYPTO 2013, LNCS Vol. 8042, pp. 531-550, 2013.

[2] A. Biryukov, C. De Canniere, A. Braeken and B. Preneel, "A Toolbox for Cryptanalysis: Linear and Affine Equivalence Algorithms", Proceedings of EUROCRYPT 2003, LNCS Vol. 2656, pp. 33-50, 2003.

[3] A. Bogdanov, L. R. Knudsen, G. Leander, F. Standaert, J. Steinberger and E. Tischhauser, "Key-Alternating Ciphers in a Provable Setting: Encryption Using a Small Number of Public Permutations", Proceedings of EUROCRYPT 2012, LNCS Vol. 7237, pp. 45-62, 2012.

[4] A. Biryukov and D. Wagner, "Advanced Slide Attacks", Proceedings of EUROCRYPT 2000, LNCS Vol. 1807, pp. 589-606, 2000.

[5] S. Chen, R. Lampe, J. Lee, Y. Seurin and J. P. Steinberger, "Minimizing the tworound Even-Mansour cipher", Proceedings of CRYPTO 2014, LNCS Vol. 8616, pp. 39-56, 2014.

[6] S. Chen and J. P. Steinberger, "Tight Security Bounds for Key-Alternating Ciphers", Proceedings of EUROCRYPT 2014, LNCS Vol. 8441, pp. 327-350, 2014.

[7] J. Daemen, "Limitations of the Even-Mansour Construction", Proceedings of ASIACRYPT 1991, LNCS Vol. 739, pp. 495-498, 1993.

[8] I. Dinur, O. Dunkelman, N. Keller and A. Shamir, " Key Recovery Attacks on 3-round Even-Mansour, 8-step LED-128, and Full AES2", Proceedings of ASIACRYPT 2013, LNCS Vol. 8269, pp. 337-356, 2013.

[9] I. Dinur, O. Dunkelman, N. Keller and A. Shamir, " Cryptanalysis of Iterated Even-Mansour Schemes with Two Keys", Proceedings of ASIACRYPT 2014, LNCS Vol. 8873, pp. 439-457, 2014.

[10] O. Dunkelman, N. Keller and A. Shamir, "Minimalism in Cryptography: The Even-Mansour Scheme Revisited", Proceedings of EUROCRYPT 2012, LNCS Vol. 7237, pp. 336-354, 2012.

[11] Y. Dai, J. Lee, B. Mennink and J. P. Steinberger,

" The Security of Multiple Encryption in the Ideal Cipher Model", Proceedings of CRYPTO 2014, LNCS Vol. 8616, pp. 20-38, 2014.

[12] S. Even and Y. Mansour, "A Construction of a Cipher From a Single Pseudorandom Permutation", Proceedings of ASIACRYPT 1991, LNCS Vol. 739, pp. 210-224, 1993.

[13] S. Even and Y. Mansour, "A Construction of a Cipher from a Single Pseudorandom Permutation", Journal of Cryptology 10(3), pp. 151-162, 1997.

[14] P. Gazi and S. Tessaro, "Efficient and Optimally Secure Key-Length Extension for Block Ciphers via Randomized Cascading", Proceedings of EUROCRYPT 2012, LNCS Vol. 7237, pp. 63-80, 2012.

[15] H. Kim, "Simplification on Even-Mansour Scheme Attacks", Journal of Information and Security, Vol. 16, No. 7, pp. 85-91, 2016.

[16] S. Noh, "A Study of DES(Data Encryption Standard) Property, Diagnosis and How to Apply Enhanced Symmetric Key Encryption Algorithm", Journal of Information and Security, Vol. 12, No. 4, pp. 85-90, 2012.

〔저 자 소 개〕

김 홍 태 (HongTae Kim)
2003년 2월 서울대 수리과학부 학사
2006년 2월 서울대 수리과학부 석사
2013년 2월 서울대 수리과학부 박사
2013년 2월 ~ 현재 공군사관학교 수학과 수학교수
email : yeskafa@naver.com